MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

SIGNIFICANCE OF THE HUMAN BEING AS AN ELEMENT IN AN INFORMATION SYSTEM: WWII FORWARD AIR CONTROLLERS AND CLOSE AIR SUPPORT

Jamie William Achée-Lieutenant, United States Navy
B.S., United States Naval Academy, 1996
Master of Science in Information Systems and Operations-March 2002
Advisors: John Arquilla, Department of Defense Analysis
Donald Stoker

This research will explore the relevance of the human being as an element in an information system. The purpose of this study is to analyze the influence technology, especially information technology, has had on the way human beings understand and use information systems. This study will look at the use of FACs and CAS in the European Theater of Operations during WWII and evaluate the technology, the doctrine and the people involved as they related to the FAC-CAS information system. Other areas that will be discussed as they relate to the development of CAS include: incremental vs. radical change, organizational culture and change, and the dynamic nature of current and future operations as they relate to information systems.

The primary research objective is to explore the answer to the following question: Based on the role of FAC in the ETO during World War II, what is the significance of the human being as an element in an information system? Secondary questions include: What are the necessary elements that make up an information system? How and where were FACs used and were they effective? What were the information systems used by the FACs and were they effective? Last, what implications do the findings of this research have for current technologies, organizational structure and the interaction between human beings and information systems in U.S. military operations?

KEYWORDS: Information, Information Systems (IS), Information Technology, Forward Air Controllers (FAC), Close Air Support (CAS), Human Element of IS, Revolution in Military Affairs (RMA), World War Two (WWII), Precision Guided Munitions (PGM), System of Systems

MULTILEVEL SECURITY REQUIREMENTS FOR A CARRIER BATTLE GROUP OPERATING ENVIRONMENT

Vincent D. Anderson-Lieutenant Commander, United States Navy
B.S., University of New Mexico, 1988
Master of Science in Information Systems and Operations-March 2002
and
Richard R. Barber-Lieutenant, United States Navy
B.S., Pennsylvania State University, 1996
Master of Science in Information Systems and Operations-March 2002
Advisor: Bret Michael, Department of Computer Science
Second Reader: LCDR Raymond Buettner, USN, Department of Information Sciences

This thesis presents and evaluates the existing technical and procedural framework supporting information sharing and processing in a multilevel security environment, identifying both the positive and negative aspects of each. The focus is on comparing existing systems against attributes and capabilities desired in

an ideal information-sharing system. This permits determination of the required configuration improvements necessary to promote timely and accurate information dissemination, and the associated metrics by which such multilevel data flow would be measured. Concurrently, this thesis presents and evaluates the existing carrier battle group information-processing procedures that govern information flow among end-users and myriad database managers. The goal is to identify the process that best enables getting the right information to the correct operational user in a timely manner to support the command and control decision-making process. Having recommended technical and procedural enhancements to current systems, it will then be possible to continue development toward a seamless common operating picture that is fully functional in a multilevel security environment and allows the end-user to access source databases and retrieve information appropriately labeled for use at the user's authorized classification level.

KEYWORDS: Multilevel Security, Carrier Battle Group, Common Operational Environment

POPULATION AND MAINTENANCE OF AN INTELLIGENCE DATABASE UTILIZING INTELLIGENT AGENT TECHNOLOGIES

Charles M. Carroll-Lieutenant Commander, United States Navy
B.S., University of North Carolina-Chapel Hill, 1987
Master of Science in Information Systems Operations-March 2002
Advisors: Mark E. Nissen, Graduate School of Business and Public Policy
Neil Rowe, Department of Computer Science

This thesis addresses the innovative gains of employing revolutionary software-agent technology for the automated construction and maintenance of databases. The intelligence process involves huge amounts of data and information that have varying degrees of assurance and processed intelligence must freely flow throughout the intelligence community to be effective. Many analysts maintain a database to track and collate specific data; making these databases public requires additional validation and maintenance rigor. Prior thesis work led to the design of a database to collect, organize and distribute key intelligence data, but man-hour expenditure for *manual* database construction and maintenance is often difficult to justify in the face of customer requests for finished intelligence products. A socio-technical systems approach is used to generate a high-level process redesign alternative. The feasibility of two key components within the new design is evaluated using existing agent technologies: a simple program to rank document relevance based on word clues learned from training, and a commercial product for automated entry of structured data. The results outline a clear plan and feasible technological approach for effecting dramatic improvements in this process.

KEYWORDS: Intelligent Agent, Database Construction, Database Population, Multi-agent Systems

PROCESS DEVELOPMENT FOR WEB-ENABLED DOCTRINE: USING A COMMERCIAL OFF THE SHELF (COTS) DISTRIBUTIVE COLLABORATIVE TECHNOLOGY (DCT)

Michael J. Harris-Lieutenant, United States Navy
B.B.A., Iowa State University, 1995
Master of Science in Information Systems and Operations-March 2002
and
Rachel J. Velasco-Lind-Lieutenant, United States Navy
B.S., Northern Arizona University, 1994
Master of Science in Information Systems and Operations-March 2002
Advisors: Erik Jansen, Department of Information Sciences
LCDR Raymond Buettner, USN, Department of Information Sciences

Navy Warfare Development Command has established Web-Enabled Doctrine (WED) in an effort to enable the Navy's transition from platform-centric operations to Network Centric Operations. The focus of this research is to describe, analyze, and evaluate the current process of developing Navy Doctrine and whether that process can be enhanced with a commercially available distributive collaborative technology (DCT). The goal of WED is to ensure that Navy Doctrine remains operationally relevant and directly connected with the Fleet. WED hopes to accomplish this by active Fleet participation in doctrinal

development and reducing timelines. The Chief of Naval Operations has set forth several priorities for the 21st century Navy, which include service unification, improved current and future readiness, and the leveraging of enabling technologies. Several commercially available DCT products appear promising to enable the Navy's transformation to web based doctrine development. This research focuses on one such product to determine the adaptability of a DCT to the Navy Doctrine process. The process uses an information system network that allows personnel the ability to remain readily engaged in the form of discussion groups during doctrinal development. This reduces cost, time, and incorporates lessons learned from subject matter experts in the Fleet.

KEYWORDS: Web-Enabled Doctrine, Navy Doctrine, Doctrine Development, Commercial-off-the-Shelf, Distributive Collaborative Technology

MODEL DESIGN FOR A BATTLEGROUP INTRANET USING AN UAV

Franklin R. Hubbard-Lieutenant, United States Navy
B.S., Texas A&M University, 1994
Master of Science in Information Systems and Operations-March 2002
and
Sean M Sadlier-Captain, United States Marine Corps
B.A., University of Illinois at Chicago, 1991
Master of Science in Information Technology Management-March 2002
Advisor: Alex Bordetsky, Department of Information Sciences
Second Reader: Charles Racoosin, Naval Space Systems Academic Chair

In this thesis the groundwork for an unmanned aerial vehicle (UAV) supporting the communications architecture of an U.S. Naval Battle Group is proposed. The Global Hawk UAV described in detail is used as an example of a viable system. A system using a UAV as a central node in a battle group intranet could enhance the communications within a battle group. The preliminary steps required to demonstrate this concept using a model based on the OPNET software program are defined. The model presented is the one recommended for modifying to research this concept further. Finally, the requirements for transitioning the existing model to one that can test the operational concept proposed in this thesis are given.

KEYWORDS: Modeling & Simulation Technology, Information Display and Performance Enhancement, Information Systems, Information Technology, Surface Ship Combatants

IMPLEMENTATION OF INFORMATION ASSURANCE RISK MANAGEMENT TRAINING INTO EXISTING DEPARTMENT OF THE NAVY TRAINING PIPELINES

Matthew, J. Labert-Lieutenant, United States Navy
B.S., United States Naval Academy, 1996
Master of Science in Information Systems Operations-March 2002
Advisor: Rex A. Buddenberg, Department of Information Sciences
Second Reader: LCDR Steven J. Iatrou, USN, Department of Information Sciences

With the implementation and continuing research on information systems, such as Information Technology for the 21st Century (IT-21), Navy-Marine Corps Intranet (NMCI), and "Network-Centric Warfare," there is little doubt that the Navy is becoming heavily dependent on information and information systems. Though much has been accomplished technically to protect and defend these systems, an important security issue has thus far been overlooked—the human factor.

Information Assurance Risk Management (IARM) was a proposal to standardize the way DON personnel discuss, treat, and implement information assurance. IARM addresses the human security aspect of information and information systems in a regimented way to be understandable through all levels of the DON.

To standardize the way DON personnel perceive information assurance, they must be taught what IARM is and how to use it. Can an IARM course be implemented in the DON, and if so at what level and to whom should it be taught?

KEYWORDS: Training, Information Assurance (IA), Information Assurance Risk Management (IARM)

AN ANALYSIS OF THE NAVAL FIRES NETWORK COMPONENT, TACTICAL EXPLOITATION SYSTEM-NAVY AS DEMONSTRATED DURING FLEET BATTLE EXPERIMENT-INDIA, JUNE 2001

Anthony C. Littmann-Lieutenant, United States Navy
B.S., Texas A&M University, 1996
Master of Science in Information Systems and Operations-March 2002
Advisor: William Kemple, Department of Information Sciences
Second Reader: Charles Marashian, Institute for Defense Systems Engineering and Analysis

In this thesis, the Naval Fires Network (NFN) component, Tactical Exploitation System-Navy (TES-N), is examined as an enabler of network centric warfare. During Fleet Battle Experiment-India (FBE-I), TES-N was found to support enhanced commander situational awareness and to a limited degree, to support both the hiders/finders and time sensitive targeting problems. However, the overall performance of TES-N was assessed as less than adequate. Many information technology issues were related to this assessment. The most significant ones were the satellite architecture and the associated problems using the transmission control protocol SMTP across the satellite links. They acted in concert to cause delays sometimes in excess of 20 minutes in passing a time sensitive targeting message. One of the most significant lessons learned during FBE-I concerning the network architecture was the utility in using bandwidth management devices such as PacketShaper. This thesis also discusses the manual process of target mensuration and proposes a way to make this process semi-autonomous using existing technologies. This thesis also includes a brief discussion of the information operations considerations of a wide area network such as NFN/TES-N. A guide to current precision-guided munitions is provided as an appendix.

KEYWORDS: Naval Fires Network (NFN), Tactical Exploitation System-Navy (TES-N), Fleet Battle Experiment-India (FBE-I), Network Centric Warfare (NCW), Information Technology, Information Operations, Tactical Exploitation of National Capabilities (TENCAP), Time Critical Target, Time Sensitive Target

INFORMATION MANAGEMENT AND THE BIOLOGICAL WARFARE THREAT

Antonio Martinez, II-Lieutenant, United States Navy
B.S., Texas A&M University, 1995
Master of Science in Information Systems and Operations-March 2002
Advisor: John Arquilla, Department of Defense Analysis
Second Reader: Shaun Jones, National Reconnaissance Office

This thesis explores the implications of information management of government-funded projects on national security objectives. A case study of the Human Genome Project is used to illustrate the risk of information transfer between government sources and private industry and the implications posed to the proliferation of Weapons of Mass Destruction. The issue of risk in information management is approached by developing three theoretical paradigms: the scientific paradigm, the business paradigm and the security paradigm. The findings of this thesis demonstrate an information sharing paradigm favoring full and open access to scientific data currently being practiced by the U.S. Human Genome Project.

The information gathered was acquired via open source information pertaining to the Human Genome Project and related initiatives. The purpose of this thesis was to raise awareness of the dangers in distributing information, funded and supplied by the United States. In addition, recommendations were made to increase the involvement of medical professionals and scientists in the non-proliferation efforts of current U.S. involvement.

KEYWORDS: Human Genome Project, Biological Warfare, Information Management

TOWARD AN INTERNET SERVICE PROVIDER (ISP) CENTRIC SECURITY APPROACH

Patrick D. Price-Commander, United States Navy
B.A., The Citadel, 1986
Master of Science in Information Systems and Operations-March 2002
Advisors: Timothy Levin, Department of Computer Science
Cynthia Irvine, Department of Computer Science

Individual users, businesses, and governments have become functionally dependent on the Internet's connectivity to interact at the most basic levels of social and economic intercourse. Yet self-propagating worms and distributed denial of service attacks have demonstrated that disruption of the Internet infrastructure can be quickly achieved despite the vast knowledge of vulnerabilities and readily available subscriber-based countermeasures. In part, this condition is made possible because networks continue to operate under an obsolete subscriber-centric security paradigm that is based on all end users being trusted to act appropriately. This thesis develops the idea of an Internet Service Provider (ISP)- centric security approach by examining the types, roles, security mechanisms, and operational precepts of ISPs to illustrate their functional control within the infrastructure. Denial of service and worm attacks are detailed to provide the context for an emerging set of conditions that forms the basis of the requirement for the ISP approach. This paper concludes by examining four enabling technologies currently available that, used uniformly, provide ISPs with the framework to implement Internet based security that can serve to enhance the layered defense model and invoke the tenants of best practices.

KEYWORDS: Internet Security, Internet Service Provider, Distributed Denial of Service

MAKING IO WORK: EXPLORING THE NEED FOR AN INFORMATION OPERATIONS COMMAND

Joseph A. Saegert-Lieutenant, United States Navy
B.S., Maine Maritime Academy, 1995
Master of Science in Information Systems and Operations-March 2002
Advisor: John Arquilla, Department of Defense Analysis
Second Reader: LCDR Steven Iatrou, USN, Department of Information Sciences

This thesis investigates the establishment of an Information Operations (IO) command and will stimulate further discussion and research of this issue. Concepts and definitions of Information Operations are presented to provide the reader a common framework of understanding upon which to base further discussion of IO. Current organizational structure, doctrine for execution of IO, and how IO supports national and military objectives are also presented and shortcomings examined. After consideration of several possible solutions a proposed structure for an IO command is presented and the feasibility of that structure discussed.

KEYWORDS: Information Systems, Information Operations, Information Warfare, Command and Control Warfare, Organization, Structure, Integration

SUGGESTIONS FOR SSN/ASDS IMPLEMENTATION AND TACMEMO CONSIDERATIONS

Travis C. Schweizer-Lieutenant Commander, United States Navy
B.A., Loyola Marymount University, 1990
Master of Science in Information Systems and Operations-March 2002
and
Michael L. Stephens-Lieutenant, United States Navy
B.S., Auburn University, 1996
Master of Science in Information Systems and Operations-March 2002
Advisor: Dan Boger, Department of Information Sciences
Second Reader: LCDR Ray Buettner, USN, Department of Information Sciences

Abstract is Classified.

KEYWORDS: ASDS, EHF, Global Grid, HUMINT, ISR&T, Littorals, Network-Centric Warfare, SEAL, Sensor, SIGINT, SSN, Stealth, Submarine, Submersible, TACMEMO, UUV, VSWMCM